Seguridad en la Internet de las cosas:

Firmwares, vulnerabilidades y riesgos en la rapidez del desarrollo y consumo de Internet Of Things

Álvaro Calvo del Olmo

Tutor: Carlos Hernández Gañán

Universitat Rovira i Virgili

UOC www.uoc.edu

UAB Universitat Autònoma de Barcelona

Estructura de la presentación

1. Introducción
2. Análisis de dos dispositivos
3. Comunicaciones seguras
4. Routers y dispositivos de gestión
5. Los dispositivos analizados en Internet
6. Soluciones
7. Conclusiones

1.

Introducción

Que es un IOT y su alcance en la sociedad

“

El IOT o Internet de las cosas es un nuevo concepto basado en la conexión de objetos de nuestro día a día a Internet

1. INTRODUCCIÓN

¿Que es un IOT?

Características que definen a un IOT:

- Conectan cosas en vez de personas
- Software muy dependiente del hardware
- Capacidades de procesamiento y memoria limitadas

Ejemplos:

- Frigoríficos
- Termostatos
- TVs
- Iluminación

1. INTRODUCCIÓN

Problemas conocidos de los IOTs

Algunos de los problemas conocidos:

- Desarrollo rápido de su software
- Soporte del fabricante demasiado corto
- Seguridad demasiado débil que, en muchos casos, no evita las contraseñas por defecto
- Exceso de exposición de los IOTs a Internet

“

El IIOT o Internet de las cosas Industrial relacionados con maquinaria, sistemas industriales, robots industriales, sensores ambientales, etc.

1. INTRODUCCIÓN

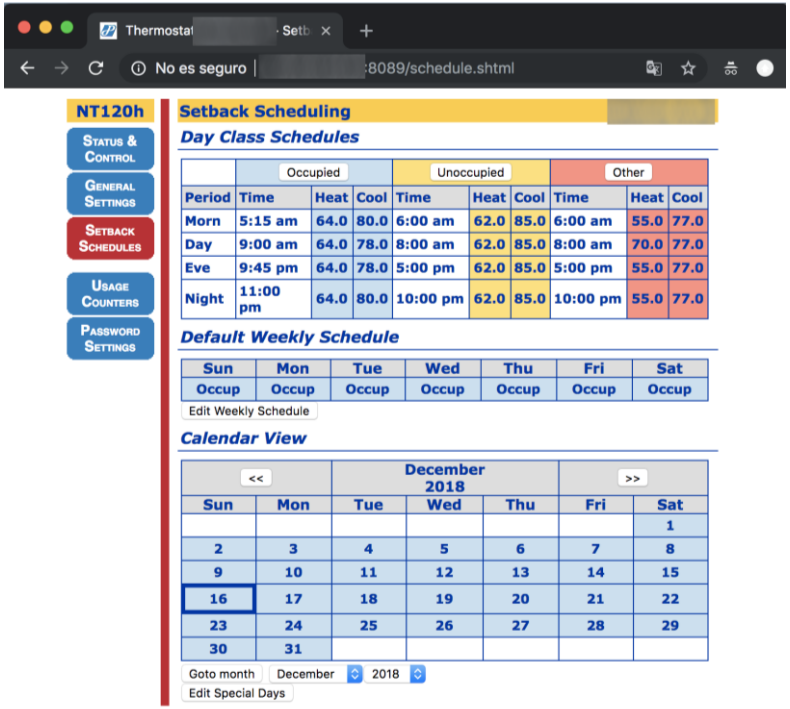
¿Donde se encuentran los IIOT?

Por la naturaleza del Industrial IIOT nos lo podemos encontrar en:

- Fábricas
- Entornos industriales
- Centrales nucleares
- Depósitos de combustible
- Estaciones meteorológicas
- ...

1. INTRODUCCIÓN

Un ejemplo de IOT: Termostato inteligente



1. INTRODUCCIÓN

Un ejemplo de IIOT: Depósitos de combustible

Depósito de combustible de una gasolinera española:

I20100
16-12-18 7:45

[redacted] S.L.

INVENTARIO EN TANQUE

PRODUCTO	TANQ	VOL	VOL CT	POR LL	ALTURA	AGUA	TEMP
1	GASOLEO C	19693	19719	31306	1029.0	0.0	13.60
2	GASOLEO B2	6396	6408	44603	466.3	0.0	13.22
3	GASOLEO A	21048	21048	29951	1081.1	0.0	15.58

“

Una Botnet es una red de dispositivos informáticos infectados donde la persona involucrada controla de manera remota para hacer aquello que desee.

1. INTRODUCCIÓN

¿Que es una botnet?

- Dispositivos que pueden fácilmente tener vulnerabilidades o debilidades de seguridad

- La utilidad para cibercriminales de tener algo a su servicio para realizar:

  - Ataques de Denegación de Servicio Distribuido
  - Envío de Spam
  - Minado de Bitcoins
  - Etc.

1. INTRODUCCIÓN

Botnet Mirai

- Botnet Mirai: famosa por sembrar el caos en Internet en el suceso del 21 de octubre de 2016
- Se atacó un servicio estratégico: servidores de DNS de Dyn
- Dyn es proveedor para distintas empresas que dan servicios conocidos
- Algunos de los servicios afectados: Amazon, Electronics Arts, GitHub, Netflix, Spotify...

2.

Análisis de dos IOT

Análisis en busca de vulnerabilidades y defectos de configuración

2. ANALISIS DE DOS IOT

- Análisis del firmware en modalidad de caja blanca para un reproductor multimedia con WIFI.
- Análisis de un amplificador de audio con WIFI en modalidad de caja negra.

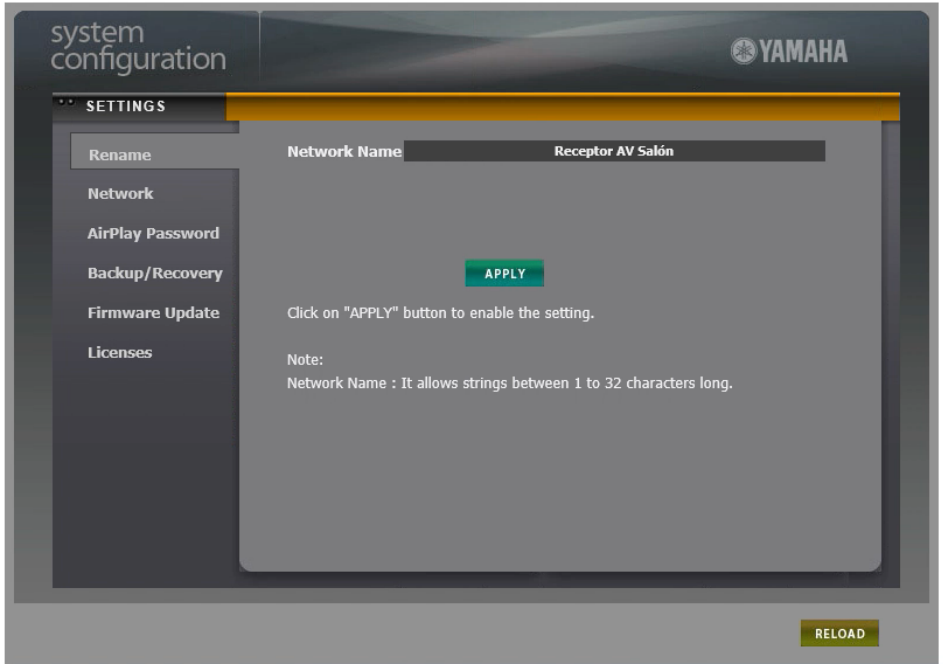
AMBOS DE CONOCIDOS FABRICANTES

VIDEOS DE PRUEBAS DE CONCEPTO DEL REPRODUCTOR MULTIMEDIA

2. ANALISIS DE DOS IOT

Amplificador de audio

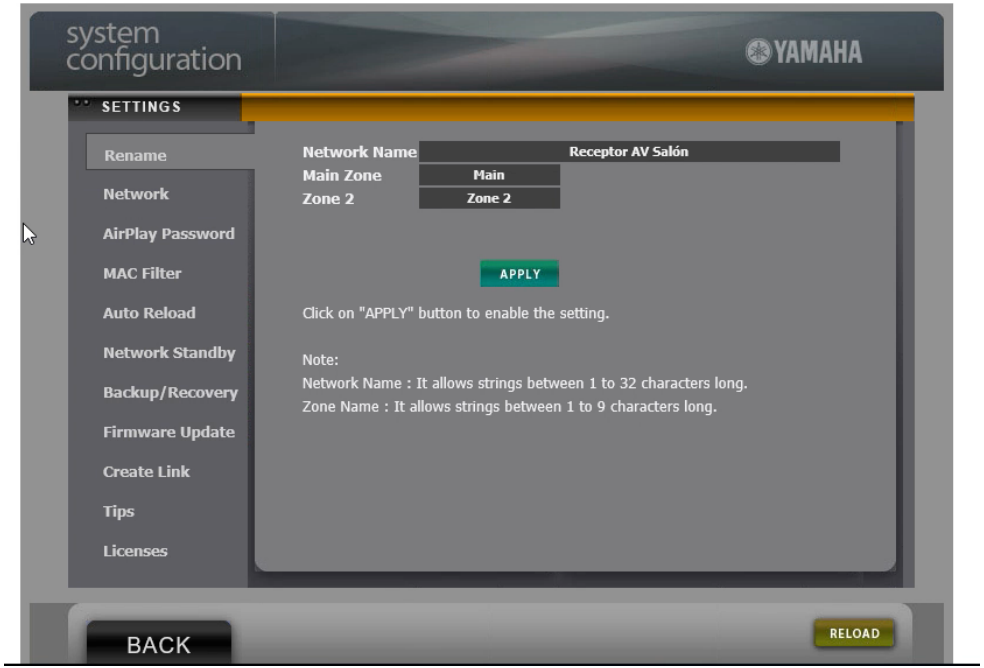
- Panel web trasero sin usuario y contraseña solo protegido por filtrado MAC
- Este panel trasero muestra mas o menos opciones de seguridad en función de la categoría del dispositivo.
- Nuestro dispositivo de pruebas es considerado de gama baja:



2. ANALISIS DE DOS IOT

Amplificador de audio

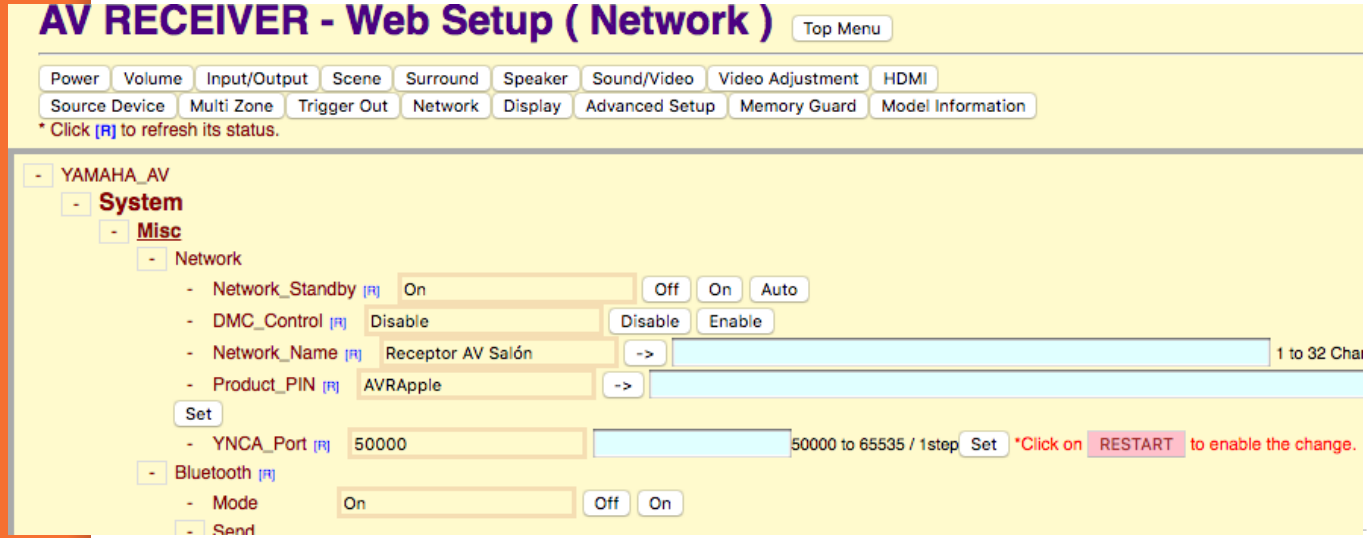
- Panel web trasero sin usuario y contraseña solo protegido por filtrado MAC
- Este panel trasero muestra mas o menos opciones de seguridad en función de la categoría del dispositivo.
- Nuestro dispositivo de pruebas es considerado de gama baja:



2. ANALISIS DE DOS IOT

Amplificador de audio

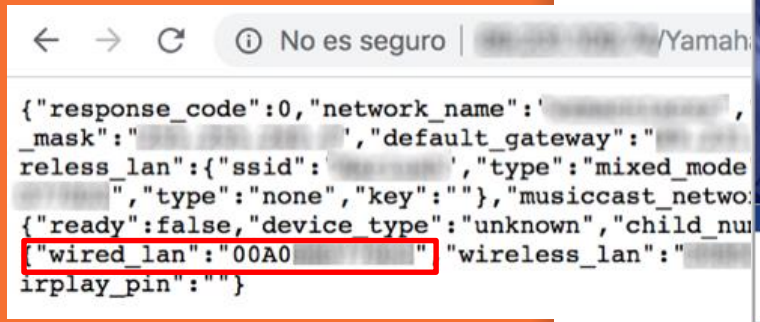
- Panel trasero donde se puede controlar todo lo que se puede desde el mando a distancia
- Sin usuario y contraseña, solo filtrado MAC
- El panel utiliza una API compartida con la app móvil llamada YNC
- Cada opción tiene una llamada vía API que puede servir para hacer nuestros propios scripts para tener el control total de sus opciones

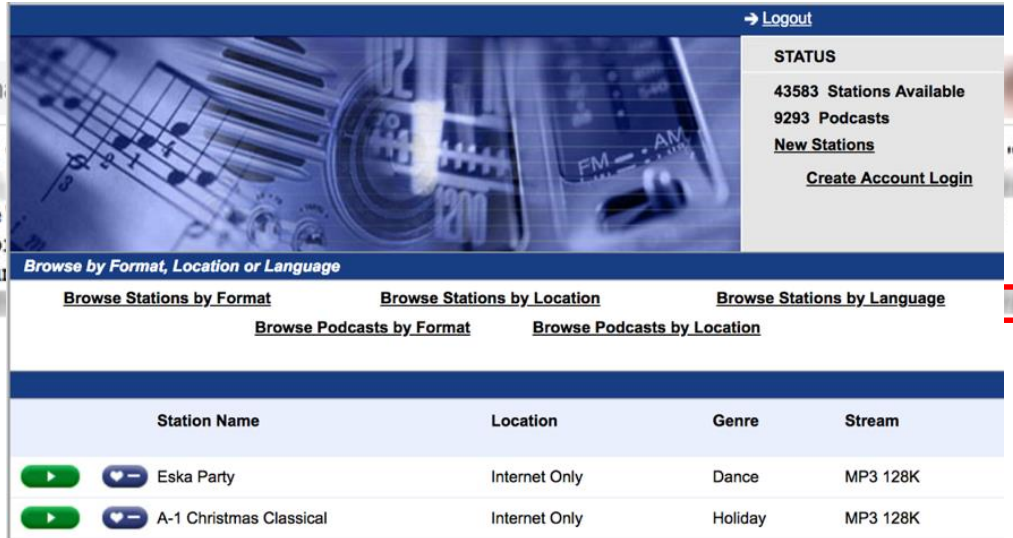


2. ANALISIS DE DOS IOT

Amplificador de audio

- Existencia de una API (YNCA) vía Telnet para hacer muchas de las cosas que con la app móvil
- Existencia de una tercera API que también tiene funciones duplicadas (YXC)
- Sobre esta ultima API YXC nos permite averiguar la dirección MAC del dispositivo
- *El login en vtuner.com puede realizarse con la dirección MAC del dispositivo lo que permite suplantar la identidad en el servicio*





VIDEO DE BLOQUEO DE VOLUMEN DE AMPLIFICADOR EN RED LAN


YAMAHA
NATURAL SOUND AV RECEIVER RX-S601
PHONES
YPAO MIC
STRAIGHT
PROGRAM
SCENE
BD/DVD
TV
NET
RADIO
AUX
AUDIO
SILENT CINEMA
VIDEO DE BLOQUEO DE VOLUMEN
DE AMPLIFICADOR EN RED LAN

3.

Comunicaciones seguras

Evitar que nos espíen el tráfico

3. COMUNICACIONES SEGURAS

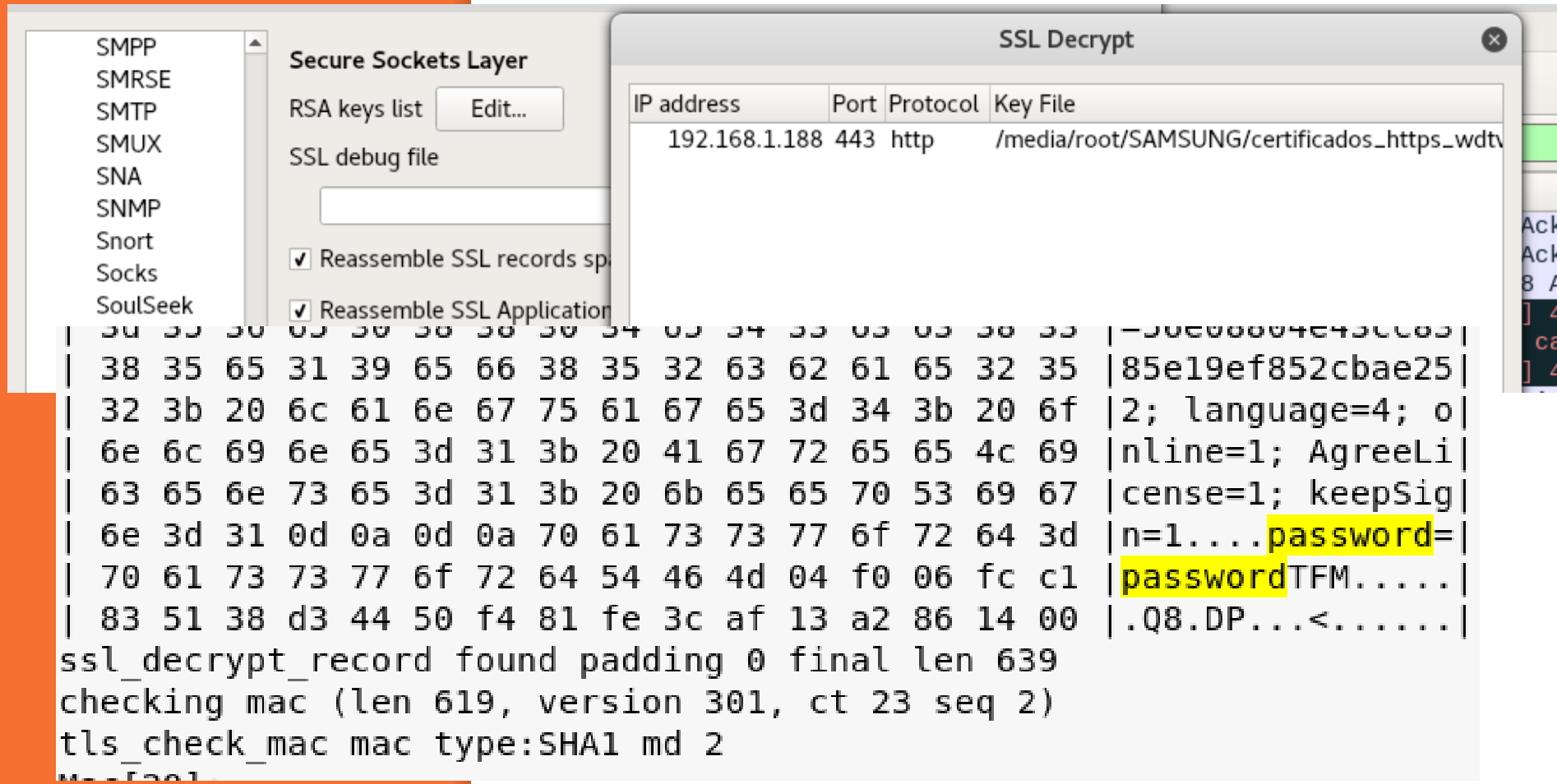
Uso de HTTPS

- Sobre HTTPS...
  - Muchos IOTs o no soportan HTTPS o lo soportan parcialmente.
  - Quienes lo soportan parcialmente, no permiten cargar un certificado propio.
  - Muchos IOTs no permiten ni regenerar el certificado autofirmado

3. COMUNICACIONES SEGURAS

Uso de HTTPS

- El amplificador: no soporta HTTPS.
- El reproductor multimedia :
  - Tiene integrada la misma clave privada para todas las unidades del mismo modelo.
  - Se puede extraer la clave privada del firmware e intervenir las comunicaciones de todas las unidades vendidas.


SMPP
SMRSE
SMTP
SMUX
SNA
SNMP
Snort
Socks
SoulSeek
Secure Sockets Layer
RSA keys list
Edit...
SSL debug file
Reassemble SSL records sp
Reassemble SSL Application
SSL Decrypt
IP address
Port
Protocol
Key File
192.168.1.188
443
http
/media/root/SAMSUNG/certificados_https_wdtv
38 35 65 31 39 65 66 38 35 32 63 62 61 65 32 35	85e19ef852cbae25
32 3b 20 6c 61 6e 67 75 61 67 65 3d 34 3b 20 6f	2; language=4; o
6e 6c 69 6e 65 3d 31 3b 20 41 67 72 65 65 4c 69	nline=1; AgreeLi
63 65 6e 73 65 3d 31 3b 20 6b 65 65 70 53 69 67	cense=1; keepSig
6e 3d 31 0d 0a 0d 0a 70 61 73 73 77 6f 72 64 3d	n=1....password=
70 61 73 73 77 6f 72 64 54 46 4d 04 f0 06 fc c1	passwordTFM.....
83 51 38 d3 44 50 f4 81 fe 3c af 13 a2 86 14 00	.Q8.DP...<......
ssl_decrypt_record found padding 0 final len 639
checking mac (len 619, version 301, ct 23 seq 2)
tls_check_mac mac type:SHA1 md 2

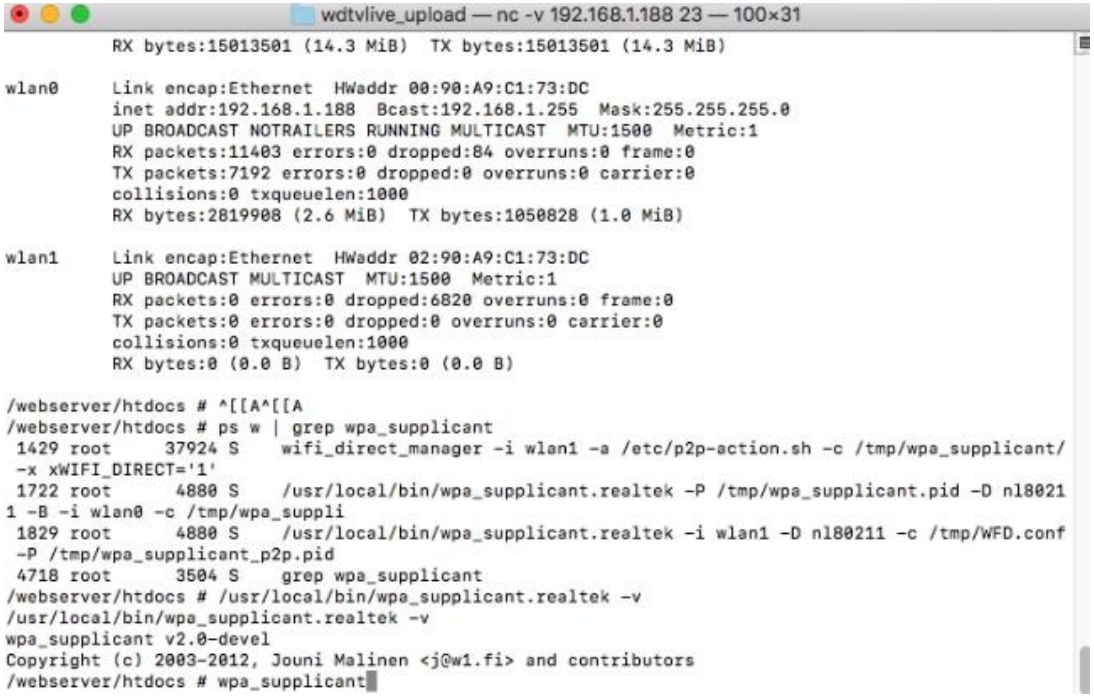
3. COMUNICACIONES SEGURAS

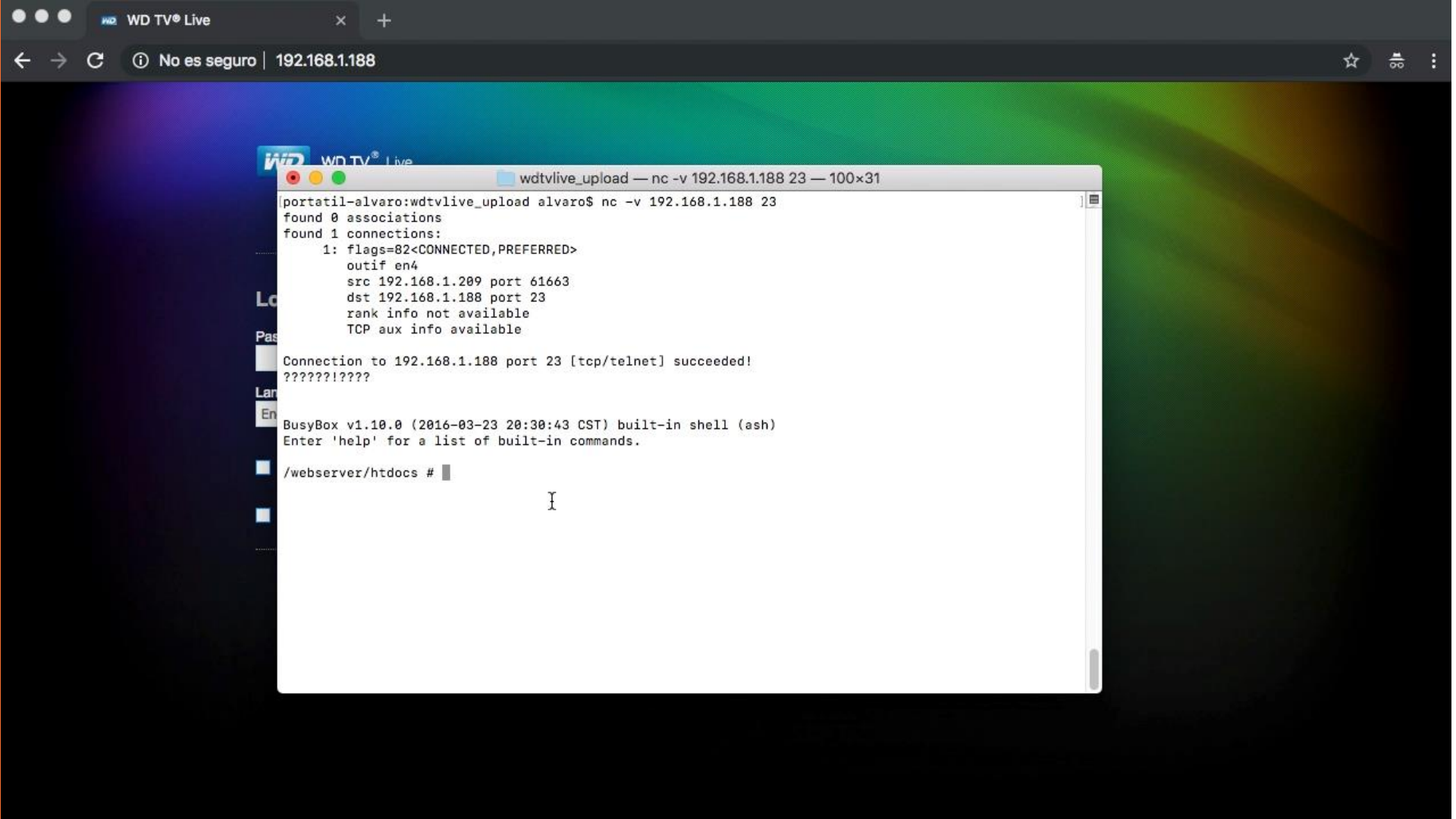
Vulnerabilidad Krack

- La vulnerabilidad Krack afecta a redes WIFI con WPA/WPA2.
- Las versiones de wpa_supplicant en Linux y Android por debajo de la versión 2.3 son vulnerables a Krack.

2.
ANALISIS DE DOS IOT

Reproductor multimedia con WIFI




WD TV® Live
No es seguro | 192.168.1.188
WD TV® Live
wdtvlive_upload — nc -v 192.168.1.188 23 — 100×31
portatil-alvaro:wdtvlive_upload alvaro$ nc -v 192.168.1.188 23
found 0 associations
found 1 connections:
1: flags=82<CONNECTED,PREFERRED>
outif en4
src 192.168.1.209 port 61663
dst 192.168.1.188 port 23
rank info not available
TCP aux info available
Connection to 192.168.1.188 port 23 [tcp/telnet] succeeded!
??????!????
BusyBox v1.10.0 (2016-03-23 20:30:43 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
/webserver/htdocs #

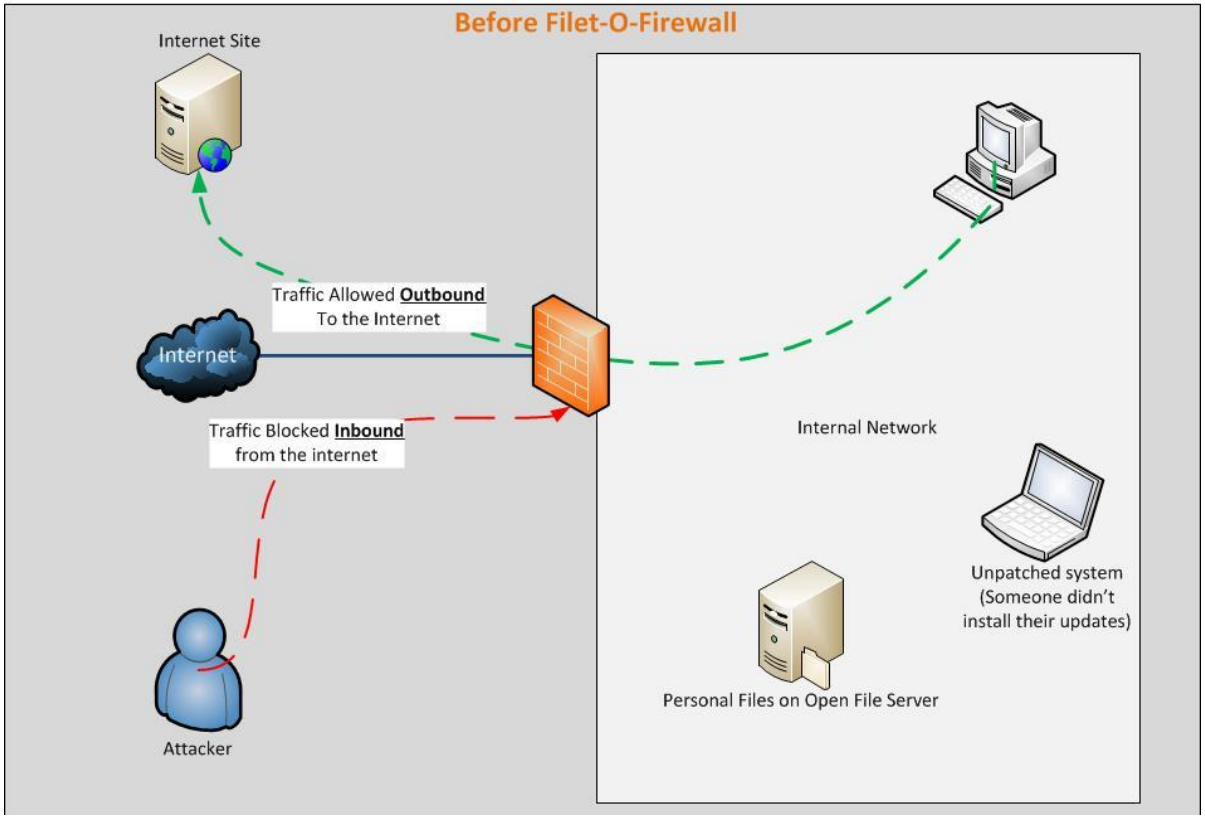
4.

Routers y dispositivos de gestión

Los alrededores de un IOT son fundamentales

4.
ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall



4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall

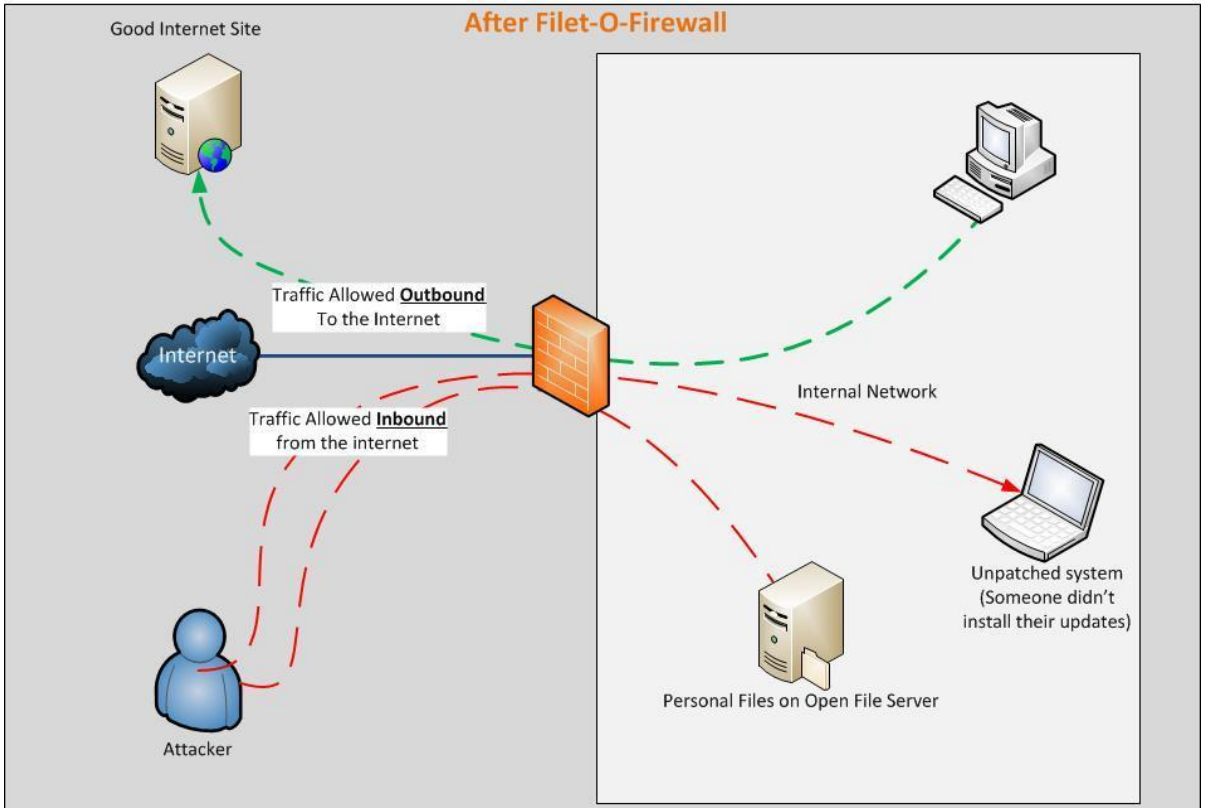
- Permitir conexiones entrantes desde Internet mediante la apertura de puertos es algo tedioso para personas no entendidas

- Gracias a IGD, un protocolo que permite que un dispositivo de la LAN “negocie” con el router la apertura automática de puertos, damos una facilidad al usuario.

- Sin embargo, IGD tiene ciertas debilidades que permiten que un programa o dispositivo no autorizado pida la apertura de puertos.

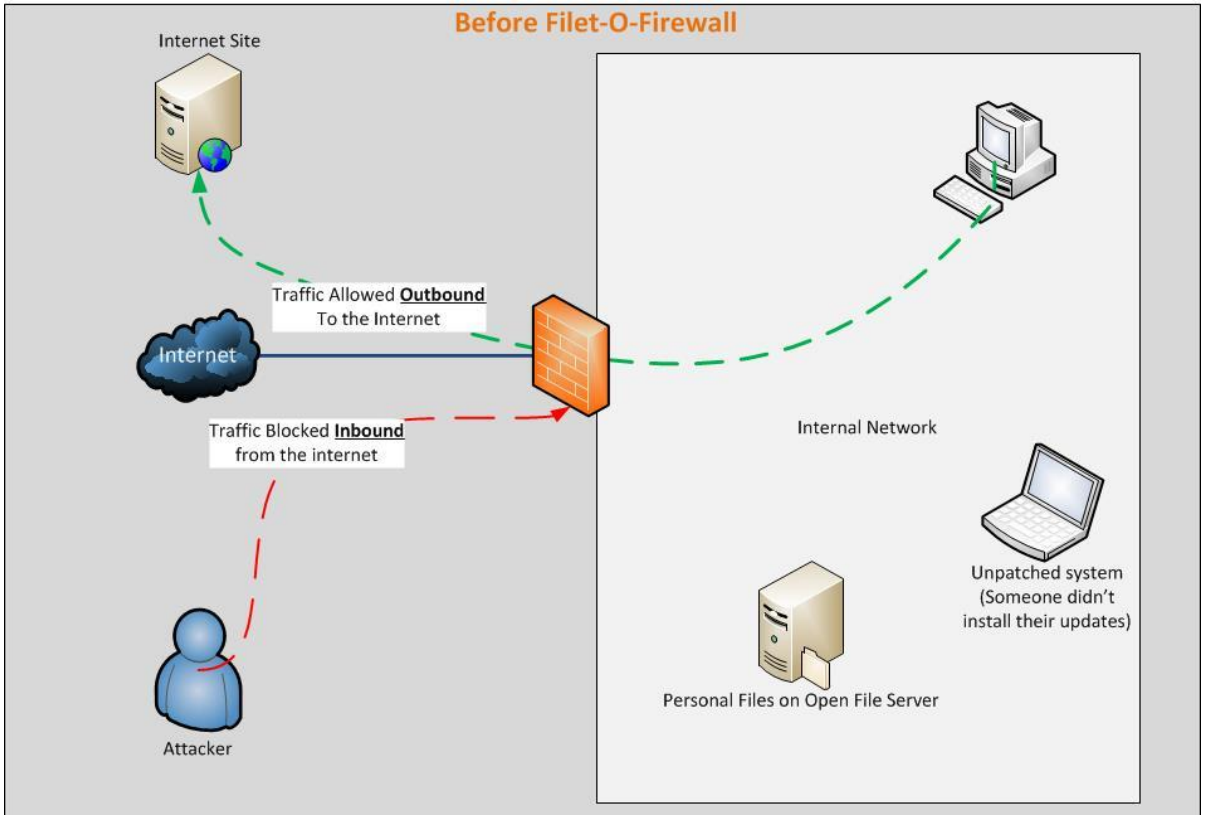
4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall



4.
ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall

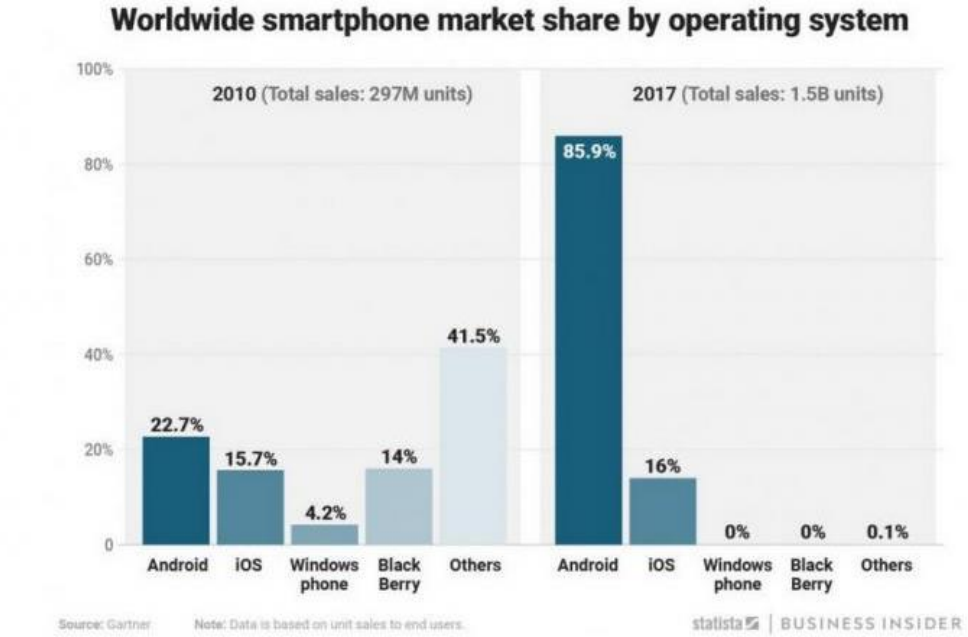


4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Sistemas operativos

- Sistemas operativos de ordenadores personales tienen ciclos de actualización mas frecuentes y con un alcance mas amplio.

- Sistemas operativos móviles (Android, iOS, etc.) tienen ciclos mas bajos de actualización, y sin embargo, son mas utilizados para manejar IOTs.



5.

Dispositivos analizados en Internet

Buscando explicaciones

5. DISPOSITIVOS ANALIZADOS EN INTERNET

Reproductor multimedia

TOTAL RESULTS

4,841

TOP COUNTRIES

United States	1,084
Canada	727
United Kingdom	560
France	267
Netherlands	186

5. DISPOSITIVOS ANALIZADOS EN INTERNET

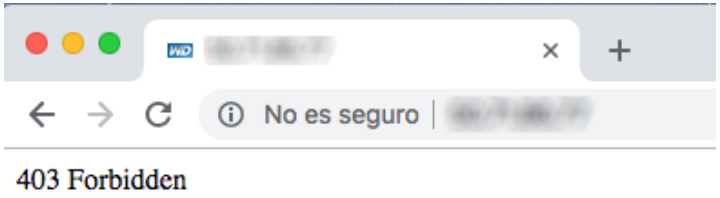
Reproductor multimedia

- Para el reproductor multimedia hubo unas decenas de IPs coincidentes con Mirai.

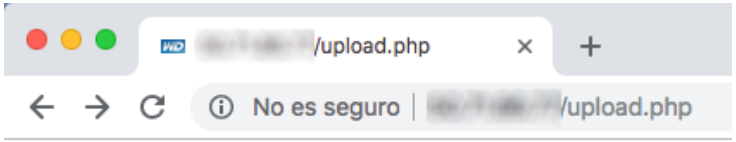
5. DISPOSITIVOS ANALIZADOS EN INTERNET

Reproductor multimedia

- Cuando se accede desde una IP externa al reproductor multimedia, el firmware lo bloquea:



- Sin embargo upload.php no tiene esa protección, como ya sabíamos, y permite subir ficheros sin autenticación:



5. DISPOSITIVOS ANALIZADOS EN INTERNET

Reproductor multimedia

- Bajo esta situación para el usuario no tiene ningún beneficio abrir el puerto al reproductor multimedia al no aportar funcionalidad.

- Sin embargo, se ha visto muchas IPs en las que upload.php no existe, es como si algo hubiese eliminado el script para no permitir subir código PHP

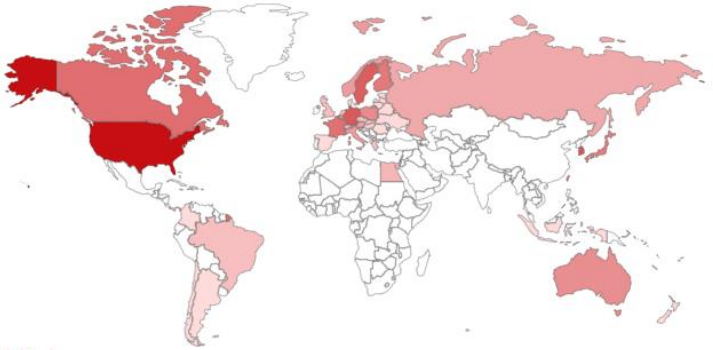
5. DISPOSITIVOS ANALIZADOS EN INTERNET

Amplificador de audio

TOTAL RESULTS

560

TOP COUNTRIES

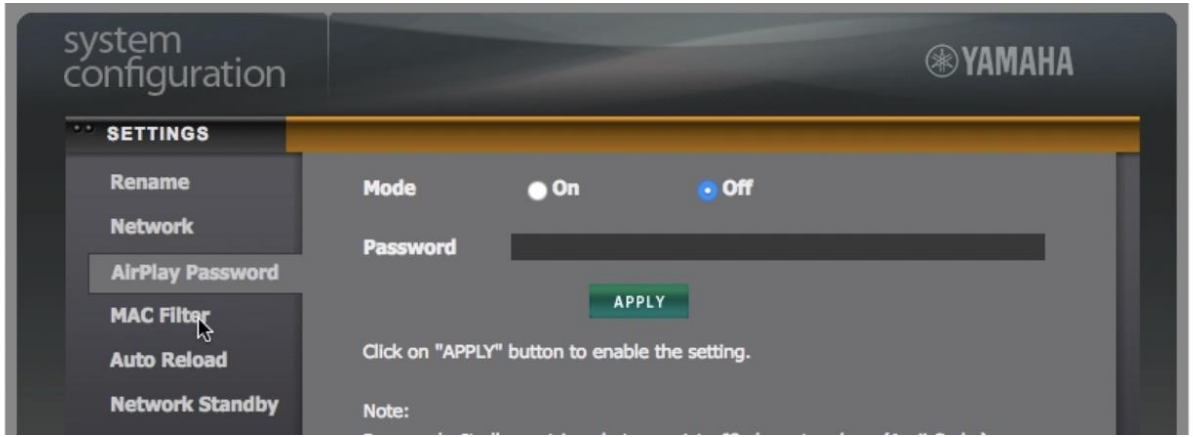


United States	173
Korea, Republic of	48
Germany	45
Sweden	41
Canada	29

5. DISPOSITIVOS ANALIZADOS EN INTERNET

Amplificador de audio

- Ninguna IP está implicada con Mirai.
- Todo apunta a que se han abierto los puertos a propósito para poder manejar el amplificador.
- Muchas de las IPs tienen abierto el puerto 5000 que permitiría el control de *Airplay* desde el exterior...
- ... donde la configuración expone que *Airplay* está además sin contraseña.

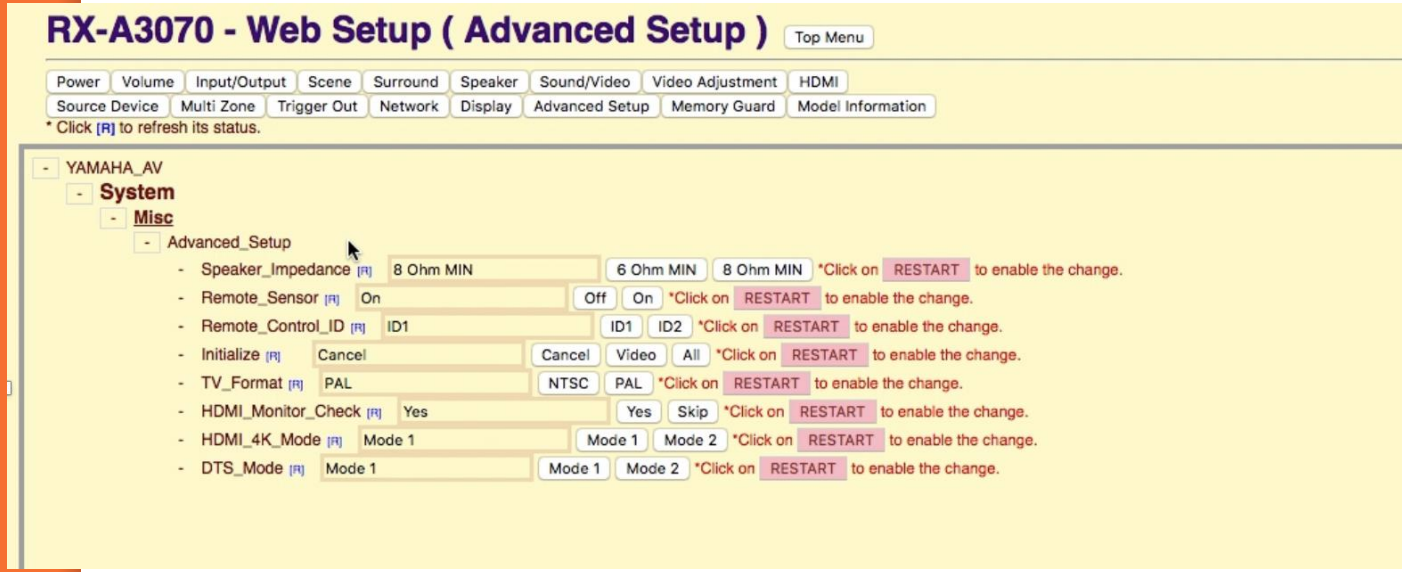


5. DISPOSITIVOS ANALIZADOS EN INTERNET

Amplificador de audio

- Facilidad de suplantar la identidad del dispositivo en vtuner.com a través de la dirección MAC

- Exposición del menú setup sin autenticación:



VIDEO DE BLOQUEO DE VOLUMEN DE AMPLIFICADOR DESDE INTERNET

6.

Soluciones

Las VPNs pueden ser parte de la solución

6. SOLUCIONES

VPN

- Uso de HTTPS siempre que sea posible para preservar las comunicaciones dentro de la red LAN

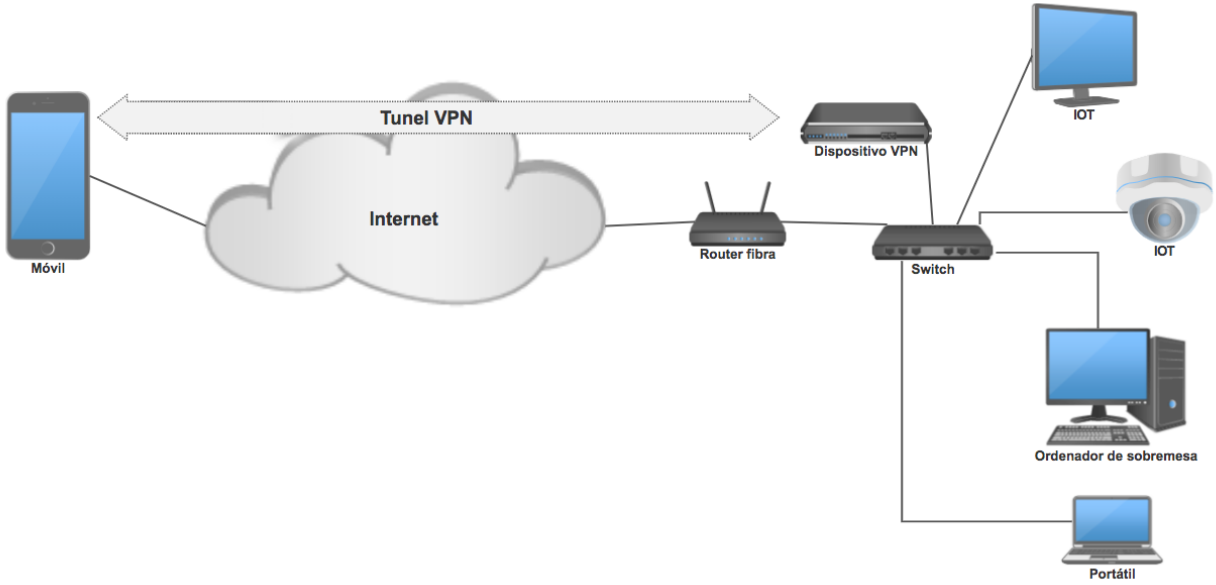
- No abrir puertos que expongan el IOT directamente al exterior....

USAR VPN

- Evitamos así que se explote cualquier vulnerabilidad del IOT directamente expuesto a Internet

6. SOLUCIONES

VPN



6. SOLUCIONES

VPN

- Con VPN los accesos desde el exterior están mejor asegurados evitando que se intercepte tráfico y credenciales de IOTs, sea cual sea la red que usemos.
- Se puede combinar perfectamente con seguridad adicional como HTTPS en el IOT, ambas formas se complementan.
- Se puede preparar un servidor VPN de IOT en Raspberry Pi a muy bajo coste donde mantenerlo actualizado.

7.

Conclusiones

7. CONCLUSIONES

- Escasez de estándares y normativas que regulen las obligaciones de los fabricantes acerca del soporte máximo en tiempo en actualizaciones, las responsabilidades y estándares mínimos de seguridad.
- Falta de concienciación a los usuarios en cuanto a configuración de IOTs.
- Los fabricantes necesitan mejorar en los IOTs una configuración de seguridad fácil a los usuarios, y no ser el usuario el que tenga que investigarlo.
- Ausencia de opciones de HTTPS para proteger las comunicaciones con IOTs

7. CONCLUSIONES

- Falta de medidas para retirar dispositivos que son declarados vulnerables sin solución

7. CONCLUSIONES

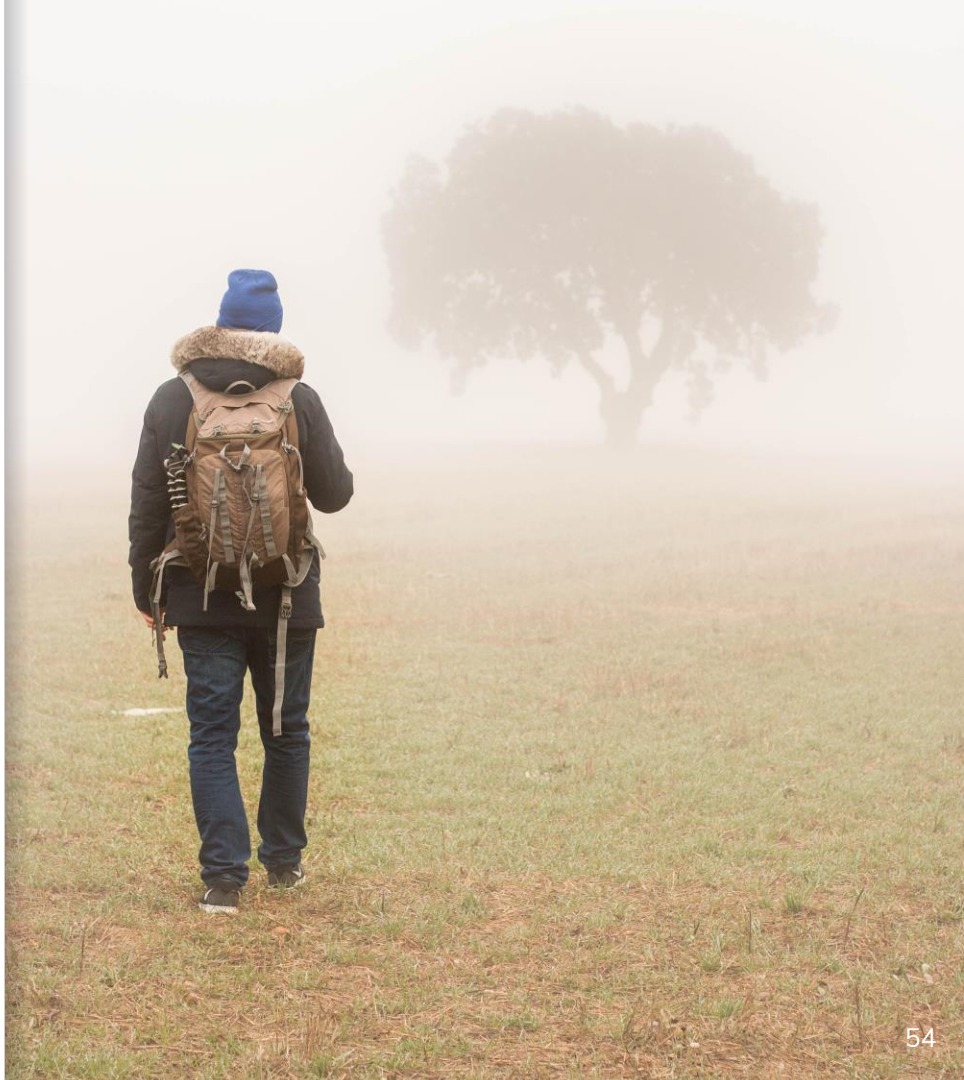
- Ausencia de mejor soporte en los sistemas operativos de los dispositivos móviles
- Falta de popularización de medidas como VPN que permitan tener una red privada entre nuestro hogar y nuestro Smartphone

7. CONCLUSIONES

- Se ha demostrado la facilidad para explorar los firmwares, tanto desde la perspectiva de caja blanca como de caja negra.
- Se ha comprobado el nivel de exposición de nuestra privacidad y nuestra seguridad personal.
- Se ha demostrado la dificultad de actualizar tantos dispositivos a raíz de la vulnerabilidad Krack en WPA
- Se ha probado la facilidad de explorar el tráfico en redes WIFI conocidas.

"No podemos resolver los problemas pensando en la misma manera que cuando los creamos"

Albert Einstein



MUCHAS GRACIAS